Homework #3 - CS6823 - Network Security

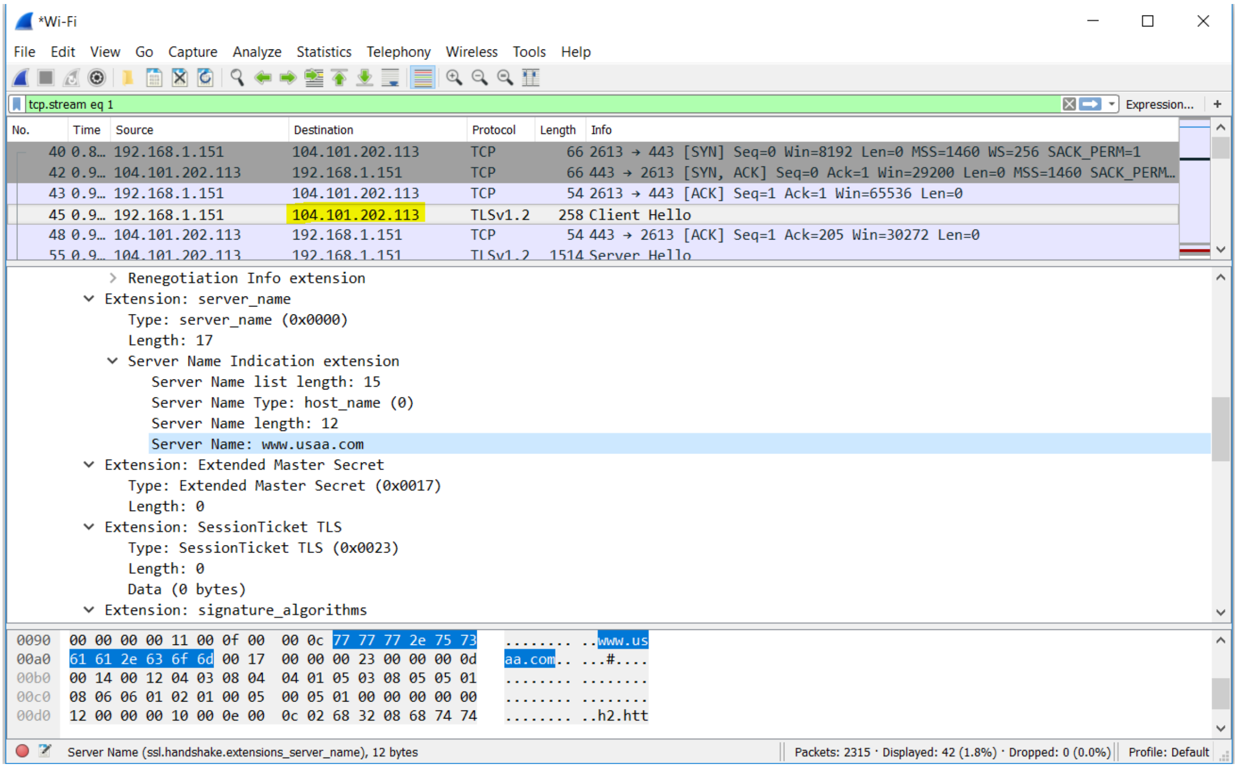
Part 1: SSL/TLS Traffic Inspection in Wireshark:

0. *Make sure you are viewing the correct connection!*

1. Proof:
   - Had a browser window with **only one HTTPS** connection to the host
   - NS lookup IP matches with the TCP SYN packet Destination IP
     ➔ Nslookup www.usaa.com

     Non-authoritative answer:

     Name: e6784.b.akamaiedge.net
     Address: 104.101.202.113
     Aliases: www.usaa.com
     wsan1.usaa.com.edgekey.net
   - Packet Capture **– Server Name** Field in Client Hello and **Destination IP = 104.101.202.113**


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

tcp.stream eq 1

```
No.   Time  Source           Destination      Protocol  Length Info
   40 0.8…  192.168.1.151    104.101.202.113  TCP         66 2613 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   42 0.9…  104.101.202.113  192.168.1.151    TCP         66 443 → 2613 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM…
   43 0.9…  192.168.1.151    104.101.202.113  TCP         54 2613 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   45 0.9…  192.168.1.151    104.101.202.113  TLSv1.2    258 Client Hello
   48 0.9…  104.101.202.113  192.168.1.151    TCP         54 443 → 2613 [ACK] Seq=1 Ack=205 Win=30272 Len=0
   55 0.9…  104.101.202.113  192.168.1.151    TLSv1.2   1514 Server Hello
```

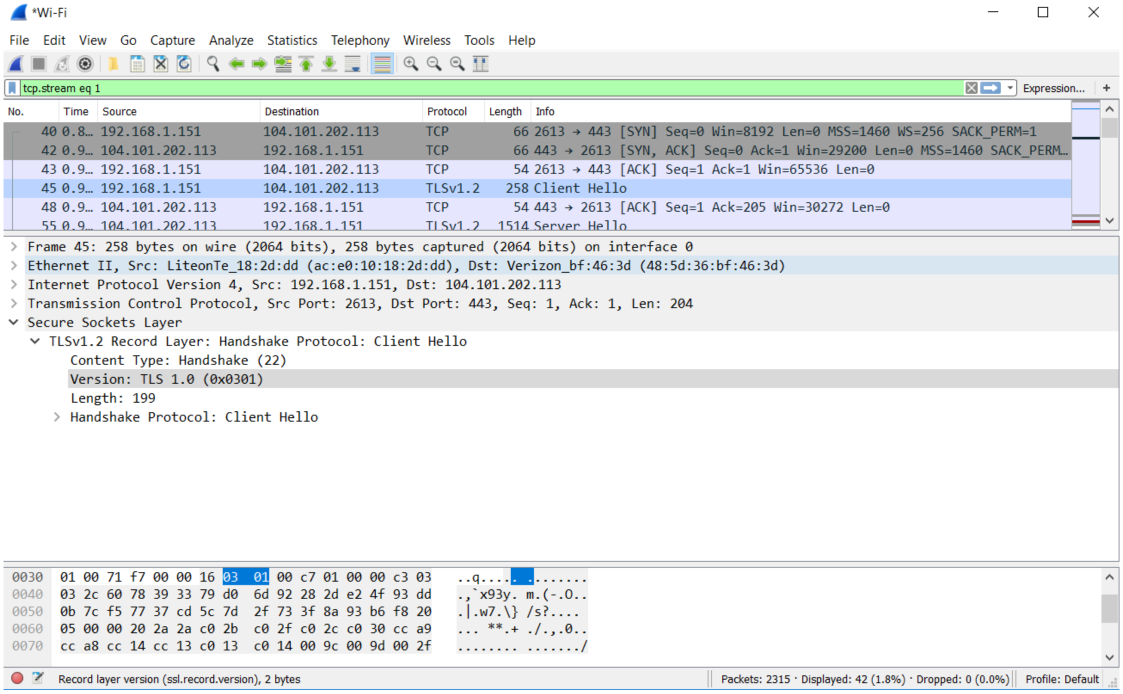
```
      > Renegotiation Info extension
    ∨ Extension: server_name
        Type: server_name (0x0000)
        Length: 17
      ∨ Server Name Indication extension
          Server Name list length: 15
          Server Name Type: host_name (0)
          Server Name length: 12
          Server Name: www.usaa.com
    ∨ Extension: Extended Master Secret
        Type: Extended Master Secret (0x0017)
        Length: 0
    ∨ Extension: SessionTicket TLS
        Type: SessionTicket TLS (0x0023)
        Length: 0
        Data (0 bytes)
    ∨ Extension: signature_algorithms
```

```
0090  00 00 00 00 11 00 0f 00  00 0c 77 77 77 2e 75 73   ........ ..www.us
00a0  61 61 2e 63 6f 6d 00 17  00 00 00 23 00 00 00 0d   aa.com.. ...#....
00b0  00 14 00 12 04 03 08 04  04 01 05 03 08 05 05 01   ........ ........
00c0  08 06 06 01 02 01 00 05  00 05 01 00 00 00 00 00   ........ ........
00d0  12 00 00 00 10 00 0e 00  0c 02 68 32 08 68 74 74   ........ ..h2.htt
```

Server Name (ssl.handshake.extensions_server_name), 12 bytes | Packets: 2315 · Displayed: 42 (1.8%) · Dropped: 0 (0.0%) | Profile: Default

2. *What's the maximum SSL/TLS version that your browser supports according to the ClientHello? Hint: Make sure you look in the ClientHello message, not the Handshake message*

   Client Version – TLS 1.0


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
tcp.stream eq 1
```

```
No.  Time   Source           Destination      Protocol  Length  Info
  40 0.8…  192.168.1.151    104.101.202.113  TCP         66 2613 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  42 0.9…  104.101.202.113  192.168.1.151    TCP         66 443 → 2613 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM…
  43 0.9…  192.168.1.151    104.101.202.113  TCP         54 2613 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  45 0.9…  192.168.1.151    104.101.202.113  TLSv1.2    258 Client Hello
  48 0.9…  104.101.202.113  192.168.1.151    TCP         54 443 → 2613 [ACK] Seq=1 Ack=205 Win=30272 Len=0
  55 0.9…  104.101.202.113  192.168.1.151    TLSv1.2   1514 Server Hello
```

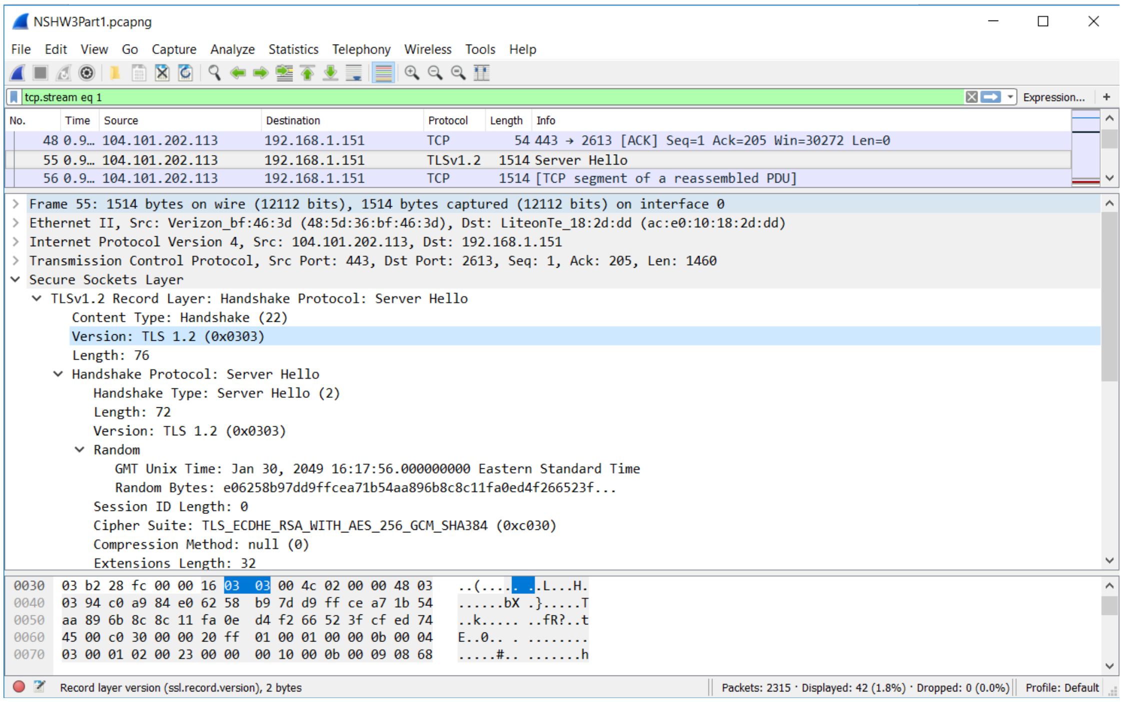
```
> Frame 45: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits) on interface 0
> Ethernet II, Src: LiteonTe_18:2d:dd (ac:e0:10:18:2d:dd), Dst: Verizon_bf:46:3d (48:5d:36:bf:46:3d)
> Internet Protocol Version 4, Src: 192.168.1.151, Dst: 104.101.202.113
> Transmission Control Protocol, Src Port: 2613, Dst Port: 443, Seq: 1, Ack: 1, Len: 204
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 199
    > Handshake Protocol: Client Hello
```

```
0030  01 00 71 f7 00 00 16 03  01 00 c7 01 00 00 c3 03   ..q..... ........
0040  03 2c 60 78 39 33 79 d0  6d 92 28 2d e2 4f 93 dd   .,`x93y. m.(-.O..
0050  0b 7c f5 77 37 cd 5c 7d  2f 73 3f 8a 93 b6 f8 20   .|.w7.\} /s?....
0060  05 00 00 20 2a 2a c0 2b  c0 2f c0 2c c0 30 cc a9   ... **.+ ./.,.0..
0070  cc a8 cc 14 cc 13 c0 13  c0 14 00 9c 00 9d 00 2f   ........ ......./
```

```
Record layer version (ssl.record.version), 2 bytes    Packets: 2315 · Displayed: 42 (1.8%) · Dropped: 0 (0.0%)    Profile: Default
```

3. *Find the "Server Hello". What version did USAA choose?*

   Server Hello – Version – TLS 1.2


NSHW3Part1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
tcp.stream eq 1
```

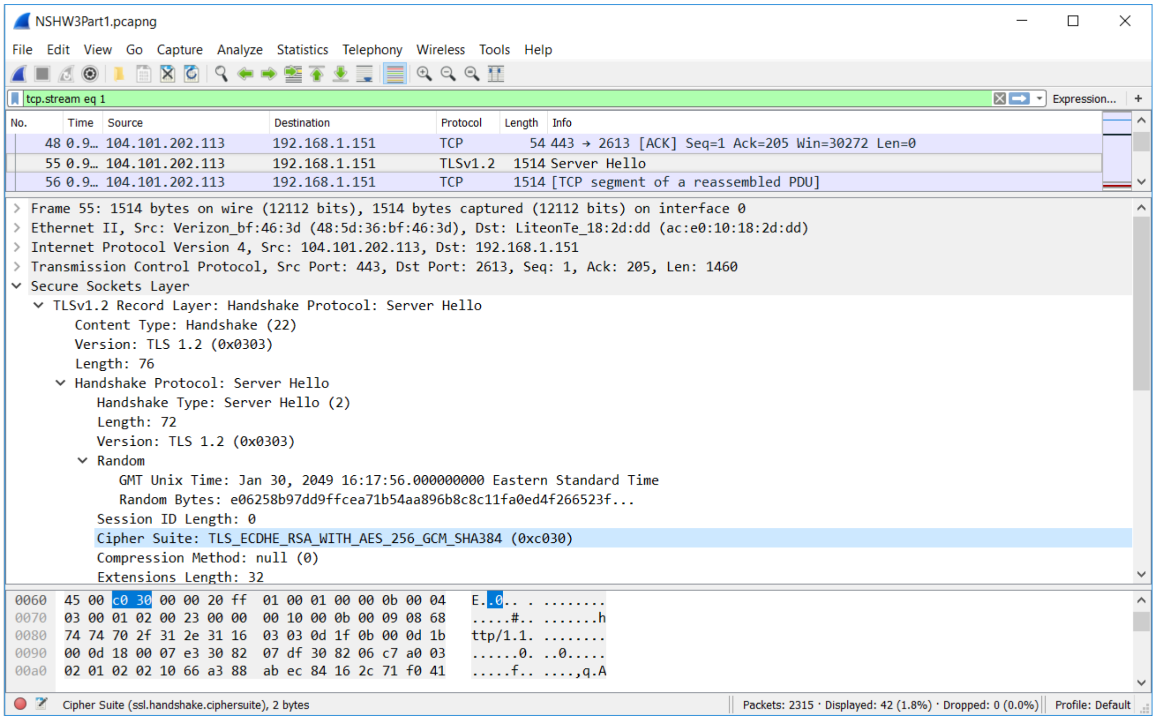
```
No.  Time   Source           Destination      Protocol  Length  Info
  48 0.9…  104.101.202.113  192.168.1.151    TCP         54 443 → 2613 [ACK] Seq=1 Ack=205 Win=30272 Len=0
  55 0.9…  104.101.202.113  192.168.1.151    TLSv1.2   1514 Server Hello
  56 0.9…  104.101.202.113  192.168.1.151    TCP       1514 [TCP segment of a reassembled PDU]
```

```
> Frame 55: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Verizon_bf:46:3d (48:5d:36:bf:46:3d), Dst: LiteonTe_18:2d:dd (ac:e0:10:18:2d:dd)
> Internet Protocol Version 4, Src: 104.101.202.113, Dst: 192.168.1.151
> Transmission Control Protocol, Src Port: 443, Dst Port: 2613, Seq: 1, Ack: 205, Len: 1460
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 76
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 72
        Version: TLS 1.2 (0x0303)
      v Random
          GMT Unix Time: Jan 30, 2049 16:17:56.000000000 Eastern Standard Time
          Random Bytes: e06258b97dd9ffcea71b54aa896b8c8c11fa0ed4f266523f...
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 32
```

```
0030  03 b2 28 fc 00 00 16 03  03 00 4c 02 00 00 48 03   ..(..... .L...H.
0040  03 94 c0 a9 84 e0 62 58  b9 7d d9 ff ce a7 1b 54   ......bX .}.....T
0050  aa 89 6b 8c 8c 11 fa 0e  d4 f2 66 52 3f cf ed 74   ..k..... ..fR?..t
0060  45 00 c0 30 00 00 20 ff  01 00 01 00 00 0b 00 04   E..0.. . ........
0070  03 00 01 02 00 23 00 00  00 10 00 0b 00 09 08 68   .....#.. .......h
```

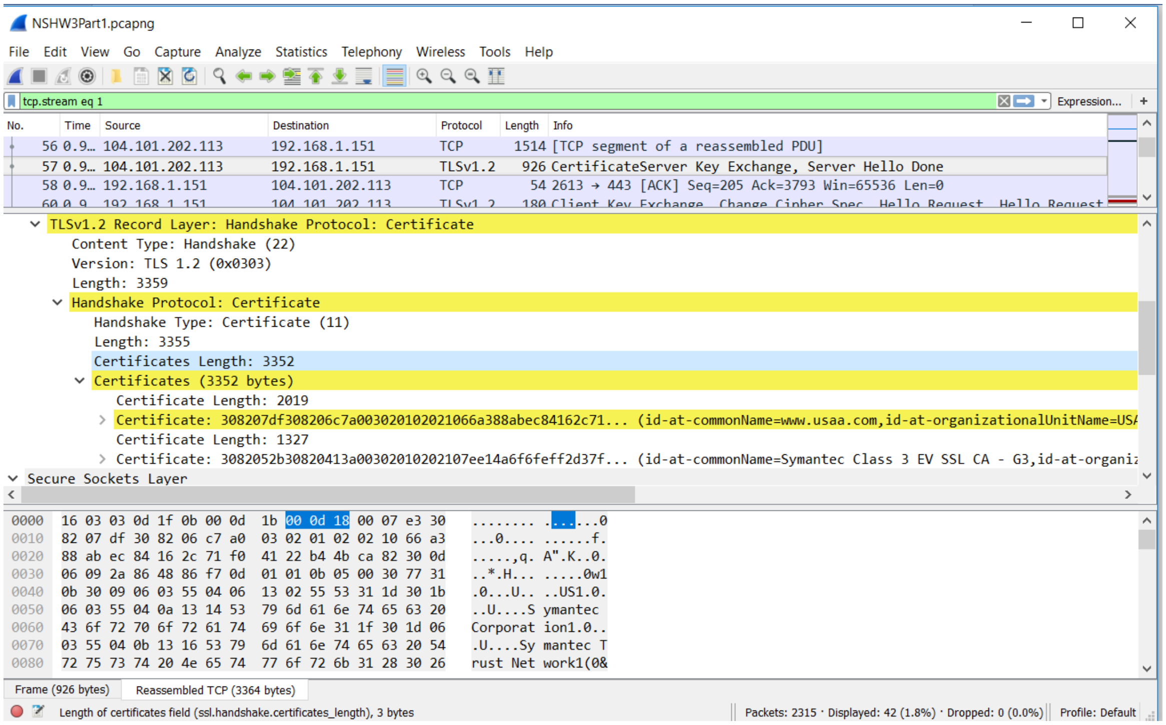
```
Record layer version (ssl.record.version), 2 bytes    Packets: 2315 · Displayed: 42 (1.8%) · Dropped: 0 (0.0%)    Profile: Default
```

4. *What Ciphersuite did USAA choose?*
   USAA Chosen Cipher Suite = TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)


NSHW3Part1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… +

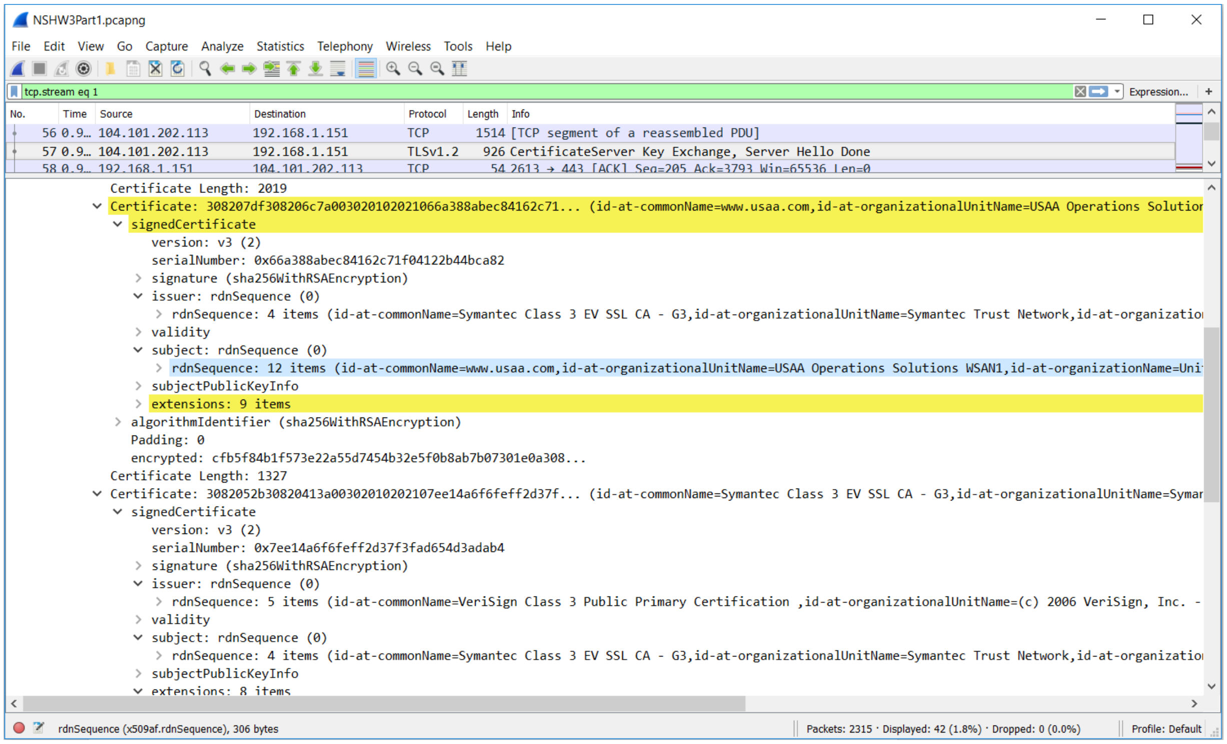
```
tcp.stream eq 1

No.   Time   Source            Destination      Protocol  Length Info
   48 0.9…  104.101.202.113   192.168.1.151    TCP          54 443 → 2613 [ACK] Seq=1 Ack=205 Win=30272 Len=0
   55 0.9…  104.101.202.113   192.168.1.151    TLSv1.2    1514 Server Hello
   56 0.9…  104.101.202.113   192.168.1.151    TCP        1514 [TCP segment of a reassembled PDU]

> Frame 55: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Verizon_bf:46:3d (48:5d:36:bf:46:3d), Dst: LiteonTe_18:2d:dd (ac:e0:10:18:2d:dd)
> Internet Protocol Version 4, Src: 104.101.202.113, Dst: 192.168.1.151
> Transmission Control Protocol, Src Port: 443, Dst Port: 2613, Seq: 1, Ack: 205, Len: 1460
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 76
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 72
        Version: TLS 1.2 (0x0303)
      v Random
          GMT Unix Time: Jan 30, 2049 16:17:56.000000000 Eastern Standard Time
          Random Bytes: e06258b97dd9ffcea71b54aa896b8c8c11fa0ed4f266523f...
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 32

0060  45 00 c0 30 00 00 20 ff  01 00 01 00 00 0b 00 04   E..0.. . ........
0070  03 00 01 02 00 23 00 00  00 10 00 0b 00 09 08 68   .....#.. .......h
0080  74 74 70 2f 31 2e 31 16  03 03 0d 1f 0b 00 0d 1b   ttp/1.1. ........
0090  00 0d 18 00 07 e3 30 82  07 df 30 82 06 c7 a0 03   ......0. ..0.....
00a0  02 01 02 02 10 66 a3 88  ab ec 84 16 2c 71 f0 41   .....f.. ....,q.A

Cipher Suite (ssl.handshake.ciphersuite), 2 bytes    Packets: 2315 · Displayed: 42 (1.8%) · Dropped: 0 (0.0%)    Profile: Default
```

5. *How many certificates did USAA send over during handshake?*
   Number Of Certificate – 2


NSHW3Part1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… +

```
tcp.stream eq 1

No.   Time   Source            Destination      Protocol  Length Info
   56 0.9…  104.101.202.113   192.168.1.151    TCP        1514 [TCP segment of a reassembled PDU]
   57 0.9…  104.101.202.113   192.168.1.151    TLSv1.2     926 CertificateServer Key Exchange, Server Hello Done
   58 0.9…  192.168.1.151     104.101.202.113  TCP          54 2613 → 443 [ACK] Seq=205 Ack=3793 Win=65536 Len=0
   60 0.9   192.168.1.151     104.101.202.113  TLSv1.2     180 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request

  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 3359
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 3355
        Certificates Length: 3352
      v Certificates (3352 bytes)
          Certificate Length: 2019
        > Certificate: 308207df308206c7a003020102021066a388abec84162c71... (id-at-commonName=www.usaa.com,id-at-organizationalUnitName=USA
          Certificate Length: 1327
        > Certificate: 3082052b30820413a00302010202107ee14a6f6feff2d37f... (id-at-commonName=Symantec Class 3 EV SSL CA - G3,id-at-organiz
v Secure Sockets Layer

0000  16 03 03 0d 1f 0b 00 0d  1b 00 0d 18 00 07 e3 30   ........ .......0
0010  82 07 df 30 82 06 c7 a0  03 02 01 02 02 10 66 a3   ...0.... ......f.
0020  88 ab ec 84 16 2c 71 f0  41 22 b4 4b ca 82 30 0d   .....,q. A".K..0.
0030  06 09 2a 86 48 86 f7 0d  01 01 0b 05 00 30 77 31   ..*.H... .....0w1
0040  0b 30 09 06 03 55 04 06  13 02 55 53 31 1d 30 1b   .0...U.. ..US1.0.
0050  06 03 55 04 0a 13 14 53  79 6d 61 6e 74 65 63 20   ..U....S ymantec 
0060  43 6f 72 70 6f 72 61 74  69 6f 6e 31 1f 30 1d 06   Corporat ion1.0..
0070  03 55 04 0b 13 16 53 79  6d 61 6e 74 65 63 20 54   .U....Sy mantec T
0080  72 75 73 74 20 4e 65 74  77 6f 72 6b 31 28 30 26   rust Net work1(0&

Frame (926 bytes)    Reassembled TCP (3364 bytes)
Length of certificates field (ssl.handshake.certificates_length), 3 bytes    Packets: 2315 · Displayed: 42 (1.8%) · Dropped: 0 (0.0%)    Profile: Default
```

6. *What's the Subject Common Name for each certificate(s)?*
   - **Certificate 1 - Common Name: www.usaa.com**
   - **Certificate 2 – Common Name: Symantec Class 3 EV SSL CA**


NSHW3Part1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
tcp.stream eq 1

No.    Time   Source           Destination      Protocol  Length Info
   56 0.9…  104.101.202.113  192.168.1.151    TCP       1514 [TCP segment of a reassembled PDU]
   57 0.9…  104.101.202.113  192.168.1.151    TLSv1.2    926 CertificateServer Key Exchange, Server Hello Done
   58 0.9…  192.168.1.151    104.101.202.113  TCP         54 2613 → 443 [ACK] Seq=205 Ack=3793 Win=65536 Len=0

        Certificate Length: 2019
      ∨ Certificate: 308207df308206c7a003020102021066a388abec84162c71... (id-at-commonName=www.usaa.com,id-at-organizationalUnitName=USAA Operations Solutio
        ∨ signedCertificate
              version: v3 (2)
              serialNumber: 0x66a388abec84162c71f04122b44bca82
            > signature (sha256WithRSAEncryption)
            ∨ issuer: rdnSequence (0)
                > rdnSequence: 4 items (id-at-commonName=Symantec Class 3 EV SSL CA - G3,id-at-organizationalUnitName=Symantec Trust Network,id-at-organizatio
            > validity
            ∨ subject: rdnSequence (0)
                > rdnSequence: 12 items (id-at-commonName=www.usaa.com,id-at-organizationalUnitName=USAA Operations Solutions WSAN1,id-at-organizationName=Uni
            > subjectPublicKeyInfo
            > extensions: 9 items
        > algorithmIdentifier (sha256WithRSAEncryption)
          Padding: 0
          encrypted: cfb5f84b1f573e22a55d7454b32e5f0b8ab7b07301e0a308...
        Certificate Length: 1327
      ∨ Certificate: 3082052b30820413a00302010202107ee14a6f6feff2d37f... (id-at-commonName=Symantec Class 3 EV SSL CA - G3,id-at-organizationalUnitName=Symar
        ∨ signedCertificate
              version: v3 (2)
              serialNumber: 0x7ee14a6f6feff2d37f3fad654d3adab4
            > signature (sha256WithRSAEncryption)
            ∨ issuer: rdnSequence (0)
                > rdnSequence: 5 items (id-at-commonName=VeriSign Class 3 Public Primary Certification ,id-at-organizationalUnitName=(c) 2006 VeriSign, Inc. -
            > validity
            ∨ subject: rdnSequence (0)
                > rdnSequence: 4 items (id-at-commonName=Symantec Class 3 EV SSL CA - G3,id-at-organizationalUnitName=Symantec Trust Network,id-at-organizatio
            > subjectPublicKeyInfo
            ∨ extensions: 8 items

rdnSequence (x509af.rdnSequence), 306 bytes    Packets: 2315 · Displayed: 42 (1.8%) · Dropped: 0 (0.0%)    Profile: Default
```

7. ***Why is the "Finished" message missing?***

   The Finished message is missing because the Encryption starts after the Change Cipher Spec message, thus not allowing Wireshark to view the packets contents.

   ->Reference:

   A Finished message is always sent immediately after a change cipher spec message to verify that the key exchange and authentication processes were successful.

   Reference: https://tools.ietf.org/html/rfc5246#section-7.4.9

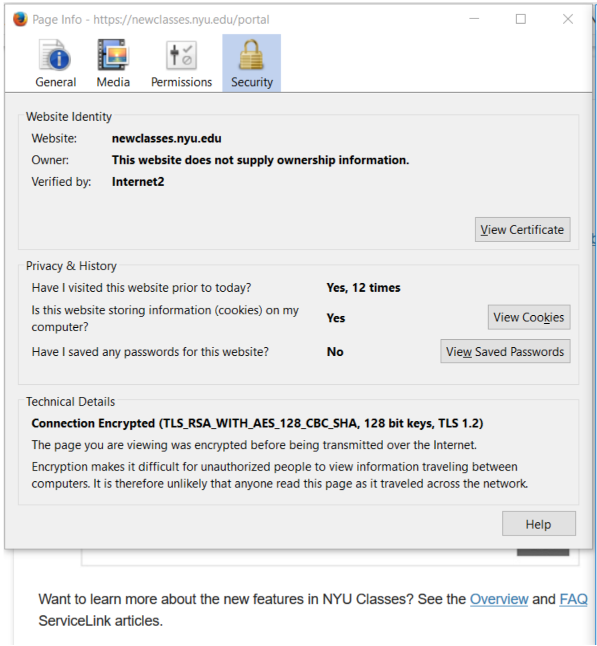
Part 2: [30 pts] SSL/TLS Inspection from web browser

	https://newclasses.nyu.edu/	https://vital.poly.edu/
What browser and OS are you using?	Mozilla Firefox	Mozilla Firefox
a. Root CA CN	USERTrust RSA Certification Authority	Let's Encrypt Authority X3
b. Subject Common Name (CN)	newclasses.nyu.edu	vital.poly.edu
c. Certificate "Valid from" date	09 April 2015	19 March 2017
d. Size of Modulus (in bits)	2048 Bits	2048 Bits

e. Value of e	65537	65537
f. Basic Constraints	Critical Is not a Certificate Authority	Critical Is not a Certificate Authority

Screenshots:

➔ ***Newclasses.nyu.edu***



Website Identity

Website: **newclasses.nyu.edu**

Owner: **This website does not supply ownership information.**

Verified by: **Internet2**

Privacy & History

Have I visited this website prior to today? **Yes, 12 times**

Is this website storing information (cookies) on my computer? **Yes**

Have I saved any passwords for this website? **No**

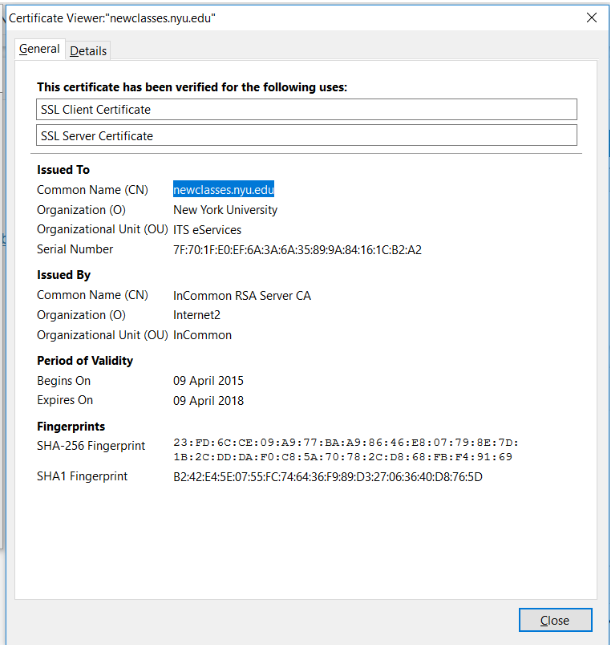
Technical Details

Connection Encrypted (TLS_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Want to learn more about the new features in NYU Classes? See the Overview and FAQ ServiceLink articles.



This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN) newclasses.nyu.edu

Organization (O) New York University

Organizational Unit (OU) ITS eServices

Serial Number 7F:70:1F:E0:EF:6A:3A:6A:35:89:9A:84:16:1C:B2:A2

Issued By

Common Name (CN) InCommon RSA Server CA

Organization (O) Internet2

Organizational Unit (OU) InCommon

Period of Validity

Begins On 09 April 2015

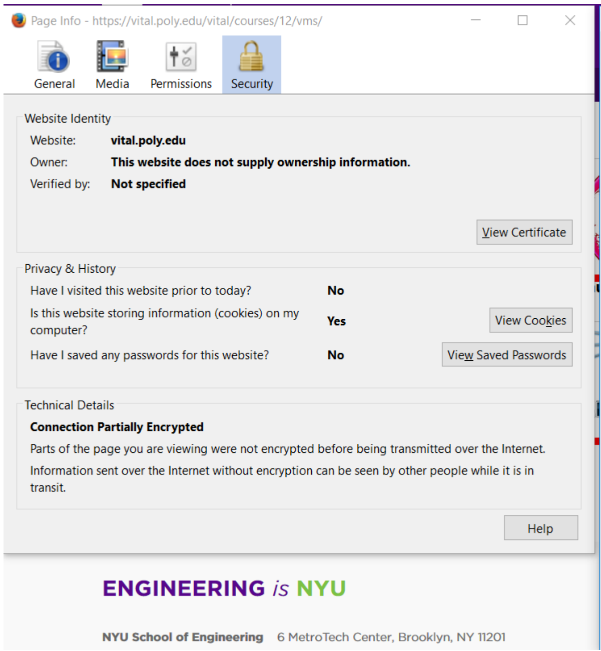
Expires On 09 April 2018

Fingerprints

SHA-256 Fingerprint 23:FD:6C:CE:09:A9:77:BA:A9:86:46:E8:07:79:8E:7D:
1B:2C:DD:DA:F0:C8:5A:70:78:2C:D8:68:FB:F4:91:69

SHA1 Fingerprint B2:42:E4:5E:07:55:FC:74:64:36:F9:89:D3:27:06:36:40:D8:76:5D

➔ ***Vital.poly.edu***


Page Info - https://vital.poly.edu/vital/courses/12/vms/
General
Media
Permissions
Security
View Certificate
View Cookies
View Saved Passwords
Help
ENGINEERING is NYU
NYU School of Engineering 6 MetroTech Center, Brooklyn, NY 11201

Website Identity

Website: **vital.poly.edu**

Owner: **This website does not supply ownership information.**

Verified by: **Not specified**

Privacy & History

Have I visited this website prior to today? **No**

Is this website storing information (cookies) on my computer? **Yes**

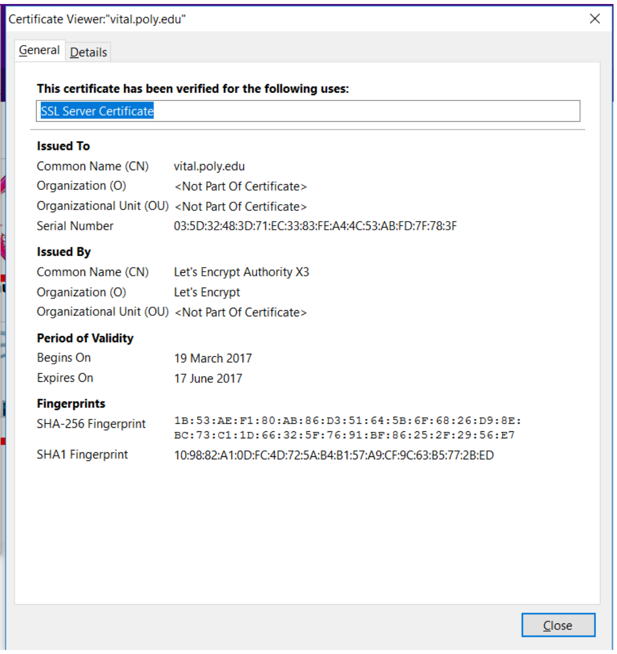
Have I saved any passwords for this website? **No**

Technical Details

Connection Partially Encrypted

Parts of the page you are viewing were not encrypted before being transmitted over the Internet.

Information sent over the Internet without encryption can be seen by other people while it is in transit.



This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN) vital.poly.edu

Organization (O) <Not Part Of Certificate>

Organizational Unit (OU) <Not Part Of Certificate>

Serial Number 03:5D:32:48:3D:71:EC:33:83:FE:A4:4C:53:AB:FD:7F:78:3F

Issued By

Common Name (CN) Let's Encrypt Authority X3

Organization (O) Let's Encrypt

Organizational Unit (OU) <Not Part Of Certificate>

Period of Validity

Begins On 19 March 2017

Expires On 17 June 2017

Fingerprints

SHA-256 Fingerprint 1B:53:AE:F1:80:AB:86:D3:51:64:5B:6F:68:26:D9:8E:
BC:73:C1:1D:66:32:5F:76:91:BF:86:25:2F:29:56:E7

SHA1 Fingerprint 10:98:82:A1:0D:FC:4D:72:5A:B4:B1:57:A9:CF:9C:63:B5:77:2B:ED

HW3 – Network Security *Srinivas Piskala Ganesh Babu – spg349 and N13138339*

Part 3: [4 pts each, total 40 pts] General Questions. All answers should be relatively short and direct.

1. ***What's the difference between HMAC and a Digital Signature?***

   HMAC:
   - Hmac Function works similar to **symmetric key** method – same key is used by both the sender and receiver.
   - Helps in Verification of **Integrity, Authenticity** but does **not help to verify Non-Repudiation** unless key information is bound to the MAC key so that one posses the key to encrypt and other to just verify
   - Vulnerable to chosen plaintext attack and forgery attack
   - Depends on the Hashing Algorithm used like MD5 or SHA

   Digital Signature:
   - Digital Signature work using public key crypto or **Asymmetric Key** method – different keys are used to encrypt and decrypt.
   - Helps in Verification of **Integrity, Authenticity and Non-Repudiation** as well by default
   - Vulnerable to forgery attack but complex to make the attack possible

2. ***How is an HMAC different than a hash?***

   Hash:
   - Used to maintain **Confidentiality** of the message
   - The Plaintext is hashed to some value which cannot be reverted back
   - Vulnerable to Chosen Plain text attack

   HMAC:
   - Used to maintain **Authenticity and Integrity** of the message.
   - The hashes are matched with the key and the message at both the sender and receiver end to verify the authenticity of the message
   - Vulnerable to Chosen Plain text attack but adds more complexity with the usage of the key – symmetric key

3. ***a. Which field of an X.509v3 certificate binds the certificate to the website's name? Be specific. (Hint: Inspect the certificate on a web browser as described in Part B.)***
   - **The Subject Common Name (CN)**
   - Example:
     - Newclasses.nyu.edu – Certificate SUBJECT Field
       - CN = newclasses.nyu.edu
       - OU = ITS eServices
       - O = New York University
       - STREET = 10 Astor Place
       - L = New York
       - S = NY
       - PostalCode = 10003
       - C = US

b. Which field of an X.509v3 certificate specifies that this certificate is a CA or an End Entity? Be specific.

- Basic Constraints – Subject Type *(CA or End Entity)*

c. Which field of an X.509v3 certificate specifies where the Certificate Revocation List (CRL) for the CA is found at? Be specific.

- CRL Distribution Point – ***Distribution Point Name*** *contains the Full Name and URL for the Certificate Revocation List.*

4. ***What is a Certificate Revocation List (CRL)?***

   Certificate Revocation List contains a **list of certificates** that have been put to a **revoked state** by the **certificate authority (CA)** who issued the Certificate and should **no longer be trusted.**

   A Certificate will be placed in a Certificate a Revocation List when:

   - **Private Key has been compromised** (Most Common Reason)
   - Improperly Issued Certificate
   - Violation of any policy

The Certificate is placed in the Revocation list **before its expiration date**.

Reference: https://en.wikipedia.org/wiki/Certificate_revocation_list

Basically it contains the list of certificates that have been blacklisted

5. ***In the X.509v3 server certificate, the Issuer CN is the same as what field in the Intermediary CA's certificate?***

   Subject CN *of the Intermediate Certificate*

6. ***Which messages are hashed in the finished message?***

   All the **Handshake messages** completed till the Change Cipher Spec (Change Cipher Spec - not included) are hashed in the Finished message

8. ***How is amazon.com authenticated to the user's browser?***

   - Verification of Server Certificate:
     - Certificate Parameters and Validity
       - Validity of the Certificate
       - The Common Name match with the Connected Channel
       - Basic Constraints for the End-Point or CA validation
   - Matches the Root CA with the trusted CA list present in the browser
   - Traverses the Issuer Field from the Endpoint to the Root CA
   - Performs Signature Verification from the Root CA Public Key to the End-Entity
     - Intermediary CA Public Key- Verify the Signature of Server (End-Entity) Certificate
     - Root CA Public Key - Verify the Signature of Intermediary Certificate

   - Intermediary CA and Root CA
     - Root CA is the certificate authority that issues the certificate - Trusted by the browser.
     - Intermediate CA is the one which verifies, signs the certificate - uses (n,e) and tries to verify the signature of the Server Certificate

9. ***How is the user's browser authenticated to amazon.com?***

   - Users Browser is **not authenticated** to the amazon.com

- Amazon.com has no idea of who the client is.
- Client identification is **not verified unless Login** is performed
- The Communication to the Server is Secure, that is the requirement.